241901077 PONSURABHI V

Ex.No: 3 **Date:15/08/2025**

PASSIVE AND ACTIVE RECONNAISSANCE

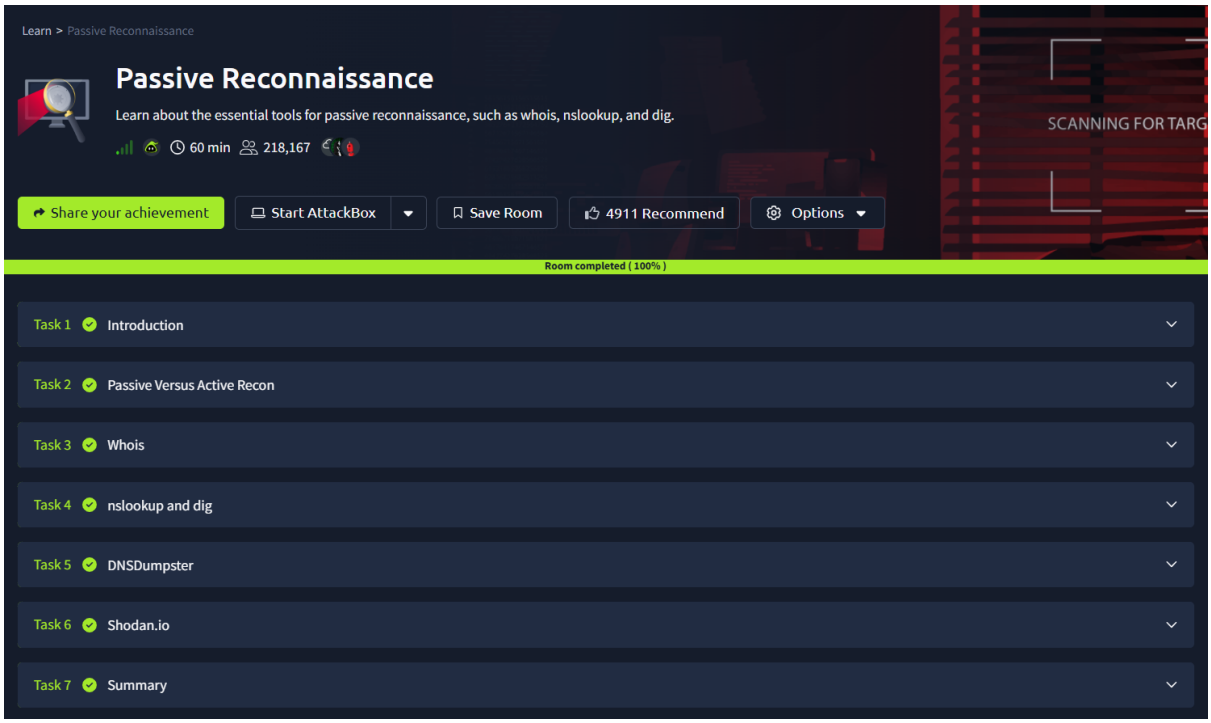
AIM:

To do perform passive and active reconnaissance in TryHackMe platform.

ALGORITHM:

1. Access the Passive reconnaissance lab in TryHackMe platform using the link below- https://tryhackme.com/r/room/passiverecon
2. Click Start AttackBox to run the instance of Kali Linux distribution.
3. Run whois command on the website tryhackme.com and gather information about it.
4. Find the IP address of tryhackme.com using nslookup and dig command.
5. Find out the subdomain of tryhackme.com using DNSDumpster command.
6. Run shodan.io to find out the details- IP address, Hosting Company, Geographical location and Server type and version.
7. Access the Active reconnaissance lab in TryHackMe platform using the link below- https://tryhackme.com/r/room/activerecon
8. Click Start AttackBox to run the instance of Kalilinux distribution.
9. Perform active reconnaissance using the commands, traceroute, ping and netcat.

241901077 PONSURABHI V

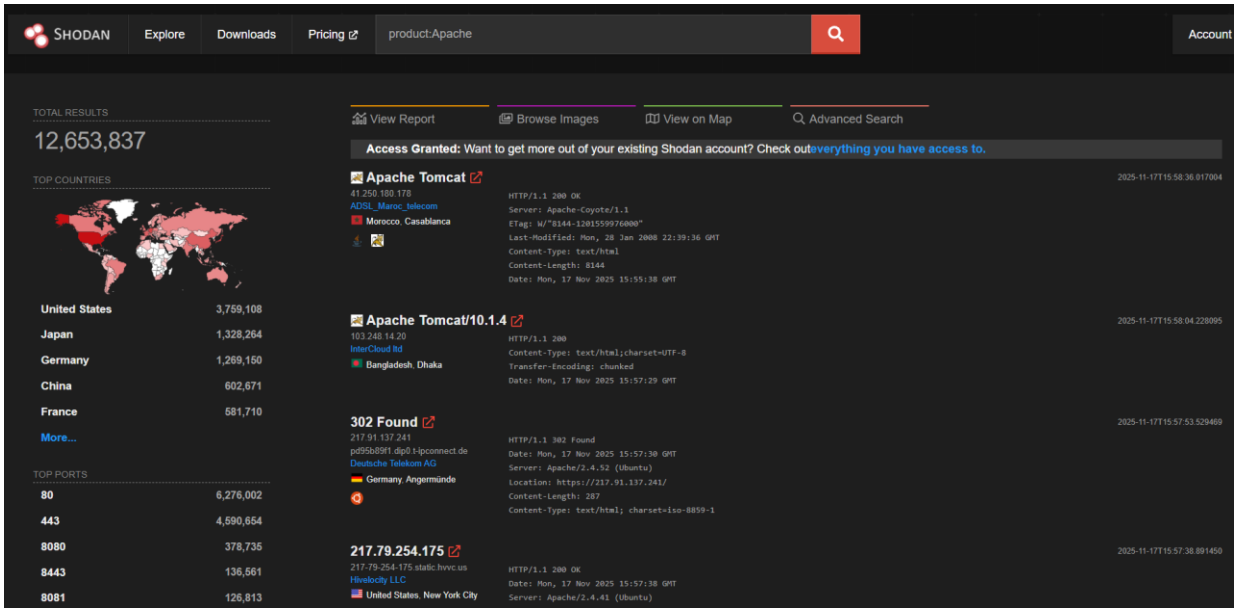


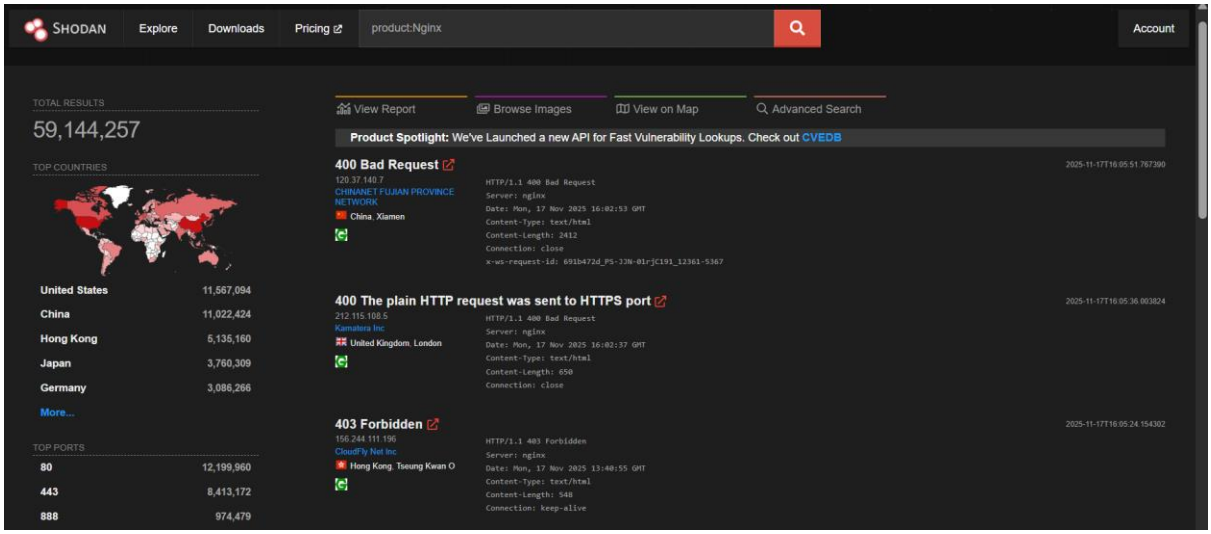

```
┌──(JackSparrow㉿Captain)-[~]
└─$ whois tryhackme.com
   Domain Name: TRYHACKME.COM
   Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namecheap.com
   Registrar URL: http://www.namecheap.com
   Updated Date: 2025-05-11T14:06:02Z
   Creation Date: 2018-07-05T19:46:15Z
   Registry Expiry Date: 2034-07-05T19:46:15Z
   Registrar: NameCheap, Inc.
   Registrar IANA ID: 1068
   Registrar Abuse Contact Email: abuse@namecheap.com
   Registrar Abuse Contact Phone: +1.6613102107
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: KIP.NS.CLOUDFLARE.COM
   Name Server: UMA.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-11-15T16:47:08Z <<<
```

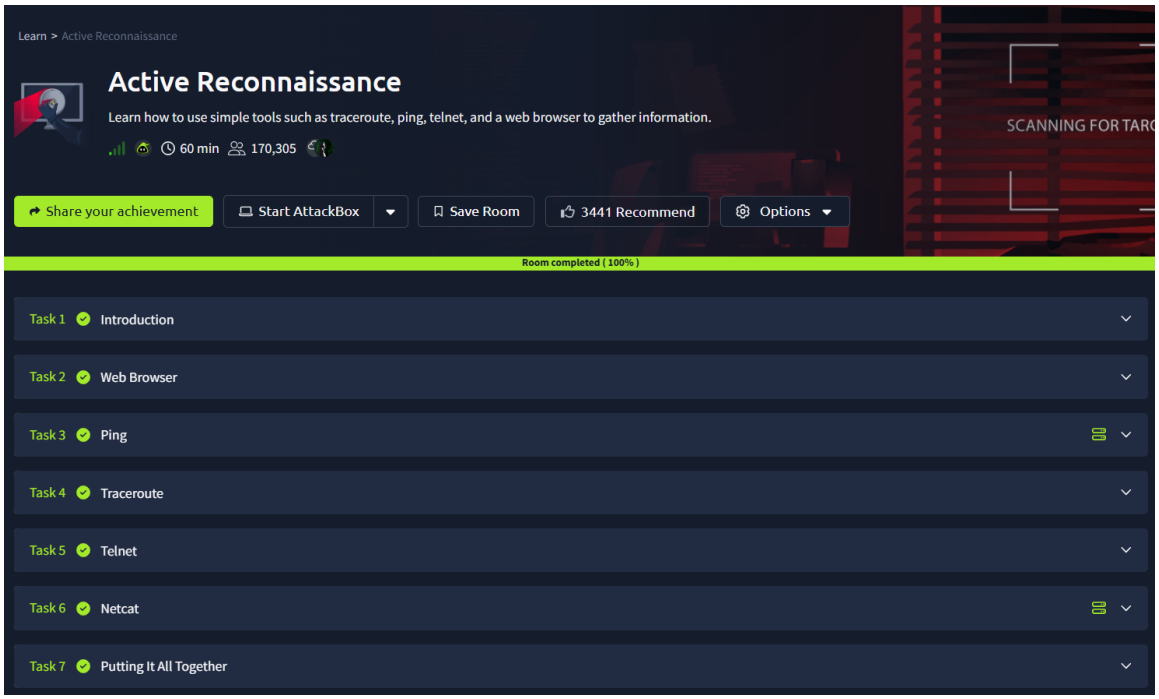
```
┌──(JackSparrow㉿Captain)-[~]
└─$ nslookup -type=MX tryhackme.com
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
tryhackme.com   mail exchanger = 1 aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt3.aspmx.l.google.com.
tryhackme.com   mail exchanger = 10 alt4.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt1.aspmx.l.google.com.
tryhackme.com   mail exchanger = 5 alt2.aspmx.l.google.com.

Authoritative answers can be found from:
```

241901077 PONSURABHI V

```
┌──(JackSparrow㉿Captain)-[~]
└─$ dig tryhackme.com MX

; <<>> DiG 9.20.11-4+b1-Debian <<>> tryhackme.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11986
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tryhackme.com.                 IN      MX

;; ANSWER SECTION:
tryhackme.com.          191     IN      MX      1 aspmx.l.google.com.
tryhackme.com.          191     IN      MX      10 alt3.aspmx.l.google.com.
tryhackme.com.          191     IN      MX      10 alt4.aspmx.l.google.com.
tryhackme.com.          191     IN      MX      5 alt1.aspmx.l.google.com.
tryhackme.com.          191     IN      MX      5 alt2.aspmx.l.google.com.

;; Query time: 39 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Sat Nov 15 22:20:16 IST 2025
;; MSG SIZE  rcvd: 157
```








```
┌──(JackSparrow㉿Captain)-[~]
└─$ traceroute tryhackme.com
traceroute to tryhackme.com (104.20.29.66), 30 hops max, 60 byte packets
 1  Captain.mshome.net (172.24.224.1)  0.934 ms  0.896 ms  0.874 ms
 2  RTK_GW (192.168.1.1)  3.782 ms  3.761 ms  4.792 ms
 3  abts-tn-dynamic-1.132.78.171.airtelbroadband.in (171.78.132.1)  6.931 ms  6.920 ms  6.906 ms
 4  125.17.36.41 (125.17.36.41)  6.968 ms  6.871 ms  6.945 ms
 5  182.79.208.203 (182.79.208.203)  6.922 ms 182.79.208.19 (182.79.208.19)  6.963 ms  6.948 ms
 6  182.79.161.171 (182.79.161.171)  8.382 ms  6.944 ms  20.323 ms
 7  162.158.52.39 (162.158.52.39)  6.334 ms 162.158.52.35 (162.158.52.35)  20.241 ms 162.158.52.39 (162.158.52.39)  6.255 ms
 8  104.20.29.66 (104.20.29.66)  6.239 ms  17.783 ms  15.676 ms
```

```
┌──(JackSparrow㉿Captain)-[~]
└─$ ping -c 5 tryhackme.com
PING tryhackme.com (172.66.164.239) 56(84) bytes of data.
64 bytes from 172.66.164.239: icmp_seq=1 ttl=58 time=10.7 ms
64 bytes from 172.66.164.239: icmp_seq=2 ttl=58 time=16.8 ms
64 bytes from 172.66.164.239: icmp_seq=3 ttl=58 time=15.4 ms
64 bytes from 172.66.164.239: icmp_seq=4 ttl=58 time=15.6 ms
64 bytes from 172.66.164.239: icmp_seq=5 ttl=58 time=15.0 ms

--- tryhackme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 10.660/14.693/16.833/2.107 ms
```

RESULT:

Thus, the passive and active reconnaissance has been performed successfully in TryHackMe platform.